1. A network multiplexing and tunneling system, comprising at least two devices connected across a network by a secure connection created at a user-level, wherein the secure connection is a single encrypted Secure Sockets Layer (SSL) Transmission Control Protocol (TCP) connection, each of the devices authenticates the other device after the secure connection is opened, and at least one of the devices multiplexes other connections through the secure connection after both the devices have been authenticated.

2. The system of claim 1, wherein the other connections are selected from a group comprising Transmission Control Protocol (TCP) and UDP (User Datagram Protocol) connections.

3. The system of claim 1, wherein the secure connection is symmetric.

4. The system of claim 1, wherein either endpoint of the secure connection can receive connection requests.

5. The system of claim 1, wherein either endpoint of the secure connection can receive data.

6. The system of claim 1, further comprising means for maintaining send buffers on each endpoint.

7. The system of claim 1, further comprising means for forwarding data through the secure connection when there are sufficient send buffers for receiving the forwarded data on the other endpoint.

8. The system of claim 1, further comprising means for queuing data received at each endpoint.

9. The system of claim 8, further comprising means for dispatching the queued data at each endpoint to its final destination.

Received from <+13106418798> at 10/31/02 3:27:39 PM [Eastern Standard Time]

10. The system of claim 9, further comprising means for acknowledging receipt of the data after the queued data is dispatched to its final destination, thereby tracking usage of buffers at the endpoint.

11. The system of claim 1, further comprising means for buffering data transmitted through the multiplexed other connections for flow control through the secure connection.

12. The system of claim 1, further comprising means for resolving domain names through the secure connection.

13. The system of claim 1, further comprising means for operating the secure connection according to a mode selected from a group comprising a standalone proxy mode, a packet filter mode, and a SOCKetS server (SOCKS) mode.

14. The system of claim 1, wherein the endpoints comprise a Portal and a Gate.

15. The system of claim 14, wherein the Gate comprises a server executed by a firewall bastion host computer.

16. The system of claim 14, wherein the Portal comprises a client executed by a user's computer.

17. The system of claim 1, further comprising means for accessing an Intranet from the Internet using the secure connection.

18. The system of claim 17, further comprising means for creating a connection from a Portal on a client computer on the Internet to a Gate on a firewall bastion host computer on the Intranet through the secure connection.

19. The system of claim 17, further comprising means for creating a connection from a Portal on a client computer on the Internet to a proxy on a firewall bastion host computer on the

Received from <+13106418798> at 10/31/02 3:27:39 PM [Eastern Standard Time]

Intranet through the secure connection and from the proxy to a Gate on a host computer on the Intranet through the secure connection.

20. The system of claim 17, further comprising means for creating a connection from a Portal on a client computer on the Internet to a packet filter on a firewall bastion host computer on the Intranet through the secure connection and from the packet filer to a Gate on a host computer on the Intranet through the secure connection.

21. The system of claim 1, further comprising means for accessing the Internet from an Intranet using the secure connection.

22. The system of claim 21, further comprising means for creating a connection from a Portal on a client computer on the Intranet to a Gate on a host computer on the Internet through the secure connection.

23. The system of claim 21, further comprising means for creating a connection from a Portal on a firewall bastion host computer on the Intranet to a host computer on the Internet through the secure connection.

24. The system of claim 21, further comprising means for creating a connection from a Portal on a client computer on the Intranet to a proxy on a firewall bastion host computer on the Intranet through the secure connection and from the proxy to a Gate on a host computer on the Internet through the secure connection.

25. The system of claim 21, further comprising means for creating a connection from a Portal on a client computer on the Intranet to a packet filter on a firewall bastion host computer on the Intranet through the secure connection and from the packet filer to a Gate on a host computer on the Internet through the secure connection.

26. The system of claim 1, further comprising means for accessing a first Intranet from a second Intranet across the Internet using the secure connection.

Received from <+13106418798> at 10/31/02 3:27:39 PM [Eastern Standard Time]

27. The system of claim 26, further comprising means for creating a connection from a Portal on a client computer on the first Intranet to a Gate on a firewall bastion host computer on the first Intranet through the secure connection, and from the Gate on the firewall bastion host computer on the first Intranet through the Internet to a Gate on a firewall bastion host computer on the second Intranet through the secure connection, and from the Gate on the firewall bastion host computer on the second Intranet to a host computer on the second Intranet through the secure connection.

28. The system of claim 1, wherein records are exchanged between the endpoints of the secure connection.

29. The system of claim 28, wherein the records are selected from a group comprising: UsherOpen, UsherOpenReply, UsherSend, UsherClose, UsherSendUdp, UsherAck, UsherEnd, and UsherRST records.

30. The system of claim 29, wherein the UsherOpen records are sent by a Portal to a Gate to open a Transmission Control Protocol (TCP) connection.

31. The system of claim 29, wherein the UsherOpenReply records are sent by a Gate to a Portal to respond to an UsherOpen record.

32. The system of claim 29, wherein the UsherSend records are sent by either a Gate or a Portal to transmit data therebetween.

33. The system of claim 29, wherein the UsherAck records are sent by either a Gate or a Portal to acknowledge a receipt of data therebetween.

34. The system of claim 29, wherein the UsherAck records are not send when data received by either a Gate or a Portal is queued prior to being forwarded to its destination.

35. The system of claim 29, wherein the UsherAck records are sent only when data received by either a Gate or a Portal has been forwarded to its destination.

Received from <+13106418798> at 10/31/02 3:27:39 PM [Eastern Standard Time]

36. The system of claim 29, wherein the UsherClose records are sent by either a Gate or a Portal to terminate a session.

37. The system of claim 29, wherein the UsherSendUdp records are sent by either a Gate or a Portal to transmit UDP (User Datagram Protocol) packets therebetween.

38. The system of claim 29, wherein the UsherEnd records are sent by either a Gate or a Portal to terminate a multiplexed other connection.

39. The system of claim 29, wherein the UsherRST records are sent by either a Gate or a Portal to reset a multiplexed other connection.

40. A transmission media communicating data via a secure connection created at a user-level between two endpoints in a network, wherein the secure connection is a single encrypted Secure Sockets Layer (SSL) Transmission Control Protocol (TCP) connection, each of the endpoints authenticates the other device after the secure connection is opened, and at least one of the endpoints multiplexes other connections through the secure connection after both the endpoints have been authenticated.

41. The transmission media of claim 40, wherein the other connections are selected from a group comprising Transmission Control Protocol (TCP) and UDP (User Datagram Protocol) connections.

42. The transmission media of claim 40, wherein the secure connection is symmetric.

43. The transmission media of claim 40, wherein either endpoint of the secure connection can receive connection requests.

44. The transmission media of claim 40, wherein either endpoint of the secure connection can receive data.

Received from <+13106418798> at 10/31/02 3:27:39 PM [Eastern Standard Time]

45. The transmission media of claim 40, further comprising maintaining send buffers on each endpoint.

46. The transmission media of claim 40, further comprising forwarding data through the secure connection when there are sufficient send buffers for receiving the forwarded data on the other endpoint.

47. The transmission media of claim 40, further comprising queuing data received at each endpoint.

48. The transmission media of claim 47, further comprising dispatching the queued data at each endpoint to its final destination.

49. The transmission media of claim 48, further comprising acknowledging receipt of the data after the queued data is dispatched to its final destination, thereby tracking usage of buffers at the endpoint.

50. The transmission media of claim 40, further comprising buffering data transmitted through the multiplexed other connections for flow control through the secure connection.

51. The transmission media of claim 40, further comprising resolving domain names through the secure connection.

52. The transmission media of claim 40, further comprising operating the secure connection according to a mode selected from a group comprising a standalone proxy mode, a packet filter mode, and a SOCKetS server (SOCKS) mode.

53. The transmission media of claim 40, wherein the endpoints comprise a Portal and a Gate.

54. The transmission media of claim 53, wherein the Gate comprises a server executed by a firewall bastion host computer.

Received from <+13106418798> at 10/31/02 3:27:39 PM [Eastern Standard Time]

55. The transmission media of claim 53, wherein the Portal comprises a client executed by a user's computer.

56. The transmission media of claim 40, further comprising accessing an Intranet from the Internet using the secure connection.

57. The transmission media of claim 56, further comprising creating a connection from a Portal on a client computer on the Internet to a Gate on a firewall bastion host computer on the Intranet through the secure connection.

58. The transmission media of claim 56, further comprising creating a connection from a Portal on a client computer on the Internet to a proxy on a firewall bastion host computer on the Intranet through the secure connection and from the proxy to a Gate on a host computer on the Intranet through the secure connection.

59. The transmission media of claim 56, further comprising creating a connection from a Portal on a client computer on the Internet to a packet filter on a firewall bastion host computer on the Intranet through the secure connection and from the packet filer to a Gate on a host computer on the Intranet through the secure connection.

60. The transmission media of claim 40, further comprising accessing the Internet from an Intranet using the secure connection.

61. The transmission media of claim 60, further comprising creating a connection from a Portal on a client computer on the Intranet to a Gate on a host computer on the Internet through the secure connection.

62. The transmission media of claim 60, further comprising creating a connection from a Portal on a firewall bastion host computer on the Intranet to a host computer on the Internet through the secure connection.

Received from <+13106418798> at 10/31/02 3:27:39 PM [Eastern Standard Time]

63. The transmission media of claim 60, further comprising creating a connection from a Portal on a client computer on the Intranet to a proxy on a firewall bastion host computer on the Intranet through the secure connection and from the proxy to a Gate on a host computer on the Internet through the secure connection.

64. The transmission media of claim 60, further comprising creating a connection from a Portal on a client computer on the Intranet to a packet filter on a firewall bastion host computer on the Intranet through the secure connection and from the packet filer to a Gate on a host computer on the Internet through the secure connection.

65. The transmission media of claim 40, further comprising accessing a first Intranet from a second Intranet across the Internet using the secure connection.

66. The transmission media of claim 65, further comprising creating a connection from a Portal on a client computer on the first Intranet to a Gate on a firewall bastion host computer on the first Intranet through the secure connection, and from the Gate on the firewall bastion host computer on the first Intranet through the Internet to a Gate on a firewall bastion host computer on the second Intranet through the secure connection, and from the Gate on the firewall bastion host computer on the second Intranet to a host computer on the second Intranet through the secure connection.

67. The transmission media of claim 40, wherein records are exchanged between the endpoints of the secure connection.

68. The transmission media of claim 67, wherein the records are selected from a group comprising: UsherOpen, UsherOpenReply, UsherSend, UsherClose, UsherSendUdp, UsherAck, UsherEnd, and UsherRST records.

69. The transmission media of claim 68, wherein the UsherOpen records are sent by a Portal to a Gate to open a Transmission Control Protocol (TCP) connection.

Received from <+13106418798> at 10/31/02 3:27:39 PM [Eastern Standard Time]

70. The transmission media of claim 68, wherein the UsherOpenReply records are sent by a Gate to a Portal to respond to an UsherOpen record.

71. The transmission media of claim 68, wherein the UsherSend records are sent by either a Gate or a Portal to transmit data therebetween.

72. The transmission media of claim 68, wherein the UsherAck records are sent by either a Gate or a Portal to acknowledge a receipt of data therebetween.

73. The transmission media of claim 68, wherein the UsherAck records are not send when data received by either a Gate or a Portal is queued prior to being forwarded to its destination.

74. The transmission media of claim 68, wherein the UsherAck records are sent only when data received by either a Gate or a Portal has been forwarded to its destination.

75. The transmission media of claim 68, wherein the UsherClose records are sent by either a Gate or a Portal to terminate a session.

76. The transmission media of claim 68, wherein the UsherSendUdp records are sent by either a Gate or a Portal to transmit UDP (User Datagram Protocol) packets therebetween.

77. The transmission media of claim 68, wherein the UsherEnd records are sent by either a Gate or a Portal to terminate a multiplexed other connection.

78. The transmission media of claim 68, wherein the UsherRST records are sent by either a Gate or a Portal to reset a multiplexed other connection.

79. A method for network multiplexing and tunneling, comprising:

(a) opening a single Transmission Control Protocol (TCP) connection at a user-level between at least two endpoints in the network;

(b) establishing a Secure Sockets Layer (SSL) over the opened Transmission Control Protocol (TCP) connection;

Received from < +13106418798 > at 10/31/02 3:27:39 PM [Eastern Standard Time]

(c) mutually authenticating each of the endpoints of the SSL TCP connection; and

(d) multiplexing other connections through the secure connection once both of the endpoints have been authenticated.

80. The method of claim 79, wherein the other connections are selected from a group comprising Transmission Control Protocol (TCP) and UDP (User Datagram Protocol) connections.

81. The method of claim 79, wherein the secure connection is symmetric.

82. The method of claim 79, wherein either endpoint of the secure connection can receive connection requests.

83. The method of claim 79, wherein either endpoint of the secure connection can receive data.

84. The method of claim 79, further comprising maintaining send buffers on each endpoint.

85. The method of claim 79, further comprising forwarding data through the secure connection when there are sufficient send buffers for receiving the forwarded data on the other endpoint.

86. The method of claim 79, further comprising queuing data received at each endpoint.

87. The method of claim 86, further comprising dispatching the queued data at each endpoint to its final destination.

88. The method of claim 87, further comprising acknowledging receipt of the data after the queued data is dispatched to its final destination, thereby tracking usage of buffers at the endpoint.

Received from <+13106418798> at 10/31/02 3:27:39 PM [Eastern Standard Time]

89. The method of claim 79, further comprising buffering data transmitted through the multiplexed other connections for flow control through the secure connection.

90. The method of claim 79, further comprising resolving domain names through the secure connection.

91. The method of claim 79, further comprising operating the secure connection according to a mode selected from a group comprising a standalone proxy mode, a packet filter mode, and a SOCKetS server (SOCKS) mode.

92. The method of claim 79, wherein the endpoints comprise a Portal and a Gate.

93. The method of claim 92, wherein the Gate comprises a server executed by a firewall bastion host computer.

94. The method of claim 92, wherein the Portal comprises a client executed by a user's computer.

95. The method of claim 79, further comprising accessing an Intranet from the Internet using the secure connection.

96. The method of claim 95, further comprising creating a connection from a Portal on a client computer on the Internet to a Gate on a firewall bastion host computer on the Intranet through the secure connection.

97. The method of claim 95, further comprising creating a connection from a Portal on a client computer on the Internet to a proxy on a firewall bastion host computer on the Intranet through the secure connection and from the proxy to a Gate on a host computer on the Intranet through the secure connection.

98. The method of claim 95, further comprising creating a connection from a Portal on a client computer on the Internet to a packet filter on a firewall bastion host computer on the Intranet

Received from < +13106418798 > at 10/31/02 3:27:39 PM [Eastern Standard Time]

through the secure connection and from the packet filer to a Gate on a host computer on the Intranet through the secure connection.

99. The method of claim 79, further comprising accessing the Internet from an Intranet using the secure connection.

100. The method of claim 99, further comprising creating a connection from a Portal on a client computer on the Intranet to a Gate on a host computer on the Internet through the secure connection.

101. The method of claim 99, further comprising creating a connection from a Portal on a firewall bastion host computer on the Intranet to a host computer on the Internet through the secure connection.

102. The method of claim 99, further comprising creating a connection from a Portal on a client computer on the Intranet to a proxy on a firewall bastion host computer on the Intranet through the secure connection and from the proxy to a Gate on a host computer on the Internet through the secure connection.

103. The method of claim 99, further comprising creating a connection from a Portal on a client computer on the Intranet to a packet filter on a firewall bastion host computer on the Intranet through the secure connection and from the packet filer to a Gate on a host computer on the Internet through the secure connection.

104. The method of claim 79, further comprising accessing a first Intranet from a second Intranet across the Internet using the secure connection.

105. The method of claim 104, further comprising creating a connection from a Portal on a client computer on the first Intranet to a Gate on a firewall bastion host computer on the first Intranet through the secure connection, and from the Gate on the firewall bastion host computer on the first Intranet through the Internet to a Gate on a firewall bastion host computer on the second

Received from <+13106418798> at 10/31/02 3:27:39 PM [Eastern Standard Time]

Intranet through the secure connection, and from the Gate on the firewall bastion host computer on the second Intranet to a host computer on the second Intranet through the secure connection.

106. The method of claim 79, wherein records are exchanged between the endpoints of the secure connection.

107. The method of claim 106, wherein the records are selected from a group comprising: UsherOpen, UsherOpenReply, UsherSend, UsherClose, UsherSendUdp, UsherAck, UsherEnd, and UsherRST records.

108. The method of claim 107, wherein the UsherOpen records are sent by a Portal to a Gate to open a Transmission Control Protocol (TCP) connection.

109. The method of claim 107, wherein the UsherOpenReply records are sent by a Gate to a Portal to respond to an UsherOpen record.

110. The method of claim 107, wherein the UsherSend records are sent by either a Gate or a Portal to transmit data therebetween.

111. The method of claim 107, wherein the UsherAck records are sent by either a Gate or a Portal to acknowledge a receipt of data therebetween.

112. The method of claim 107, wherein the UsherAck records are not send when data received by either a Gate or a Portal is queued prior to being forwarded to its destination.

113. The method of claim 107, wherein the UsherAck records are sent only when data received by either a Gate or a Portal has been forwarded to its destination.

114. The method of claim 107, wherein the UsherClose records are sent by either a Gate or a Portal to terminate a session.

Received from <+13106418798> at 10/31/02 3:27:39 PM [Eastern Standard Time]

115. The method of claim 107, wherein the UsherSendUdp records are sent by either a Gate or a Portal to transmit UDP (User Datagram Protocol) packets therebetween.

116. The method of claim 107, wherein the UsherEnd records are sent by either a Gate or a Portal to terminate a multiplexed other connection.

117. The method of claim 107, wherein the UsherRST records are sent by either a Gate or a Portal to reset a multiplexed other connection.

Received from < +13106418798 > at 10/31/02 3:27:39 PM [Eastern Standard Time]